UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	Criminal No. 1:18-cr-10436-PBS
v.	)	
AHMEDELHADI YASSIN SERAGELDIN, a/k/a AHMED SERAGELDIN, Defendant.	)	

GOVERNMENT'S SENTENCING MEMORANDUM

The United States moves this Court to sentence Defendant Serageldin to 60 months of imprisonment, a fine within the Guidelines sentencing range of $20,000 to $200,000, 36 months of supervised release, a mandatory special assessment of $100, and forfeiture. Defendant deserves this serious sentence because he deliberately endangered national security, at the very least by keeping national defense information where it was viewable and available to others, and because this sentence is the minimum necessary to reflect the seriousness of the offense, to promote respect for the law, to provide just punishment, and to deter others with security clearances from acting similarly.

The Sentencing Guidelines

As noted in the plea agreement, Defendant's base offense level is 24, because he retained national defense information that was classified at the CONFIDENTIAL and SECRET levels. USSG § 2M3.3. His offense level is increased by 2 levels, to 26, because he abused a position of trust with a security clearance and access to classified materials. USSG § 3B1.3. His offense level is increased by an additional 2 levels, to 28, because he willfully obstructed and impeded,

and attempted to obstruct and impede, the investigation of his national defense information offenses, by lying to multiple people he knew would communicate with law enforcement and by seeking to conceal and destroy records sought during the investigation. His resulting offense level is therefore 28, which is then reduced by 3 levels for accepting responsibility by pleading guilty before trial. USSG § 3E1.1. His total adjusted offense level is therefore 25.

The Sentencing Guidelines act best when they serve as a qualitative measure of moral culpability and resulting harm. They do a good job of measuring Defendant's moral culpability and resulting harm here. The high base offense of 24 rightly accounts for the seriousness of jeopardizing and refusing to return national defense information, and it also rightly takes into account that information's security classification level. The Guidelines' 2-level increase for abuse of a position of trust also rightly accounts for Defendant's violation of his written promises to keep national defense information secure and not to expose it to risk of loss or theft. Not everybody who violates 18 U.S.C. § 793(e) has made such promises; Defendant did and thus he has higher moral culpability for breaking them. The Guidelines' 2-level increase for obstruction of justice also rightly punishes Defendant's attempts to evade detection and punishment. Not everybody who violates 18 U.S.C. § 793(e) tries to cover up his crime. But Defendant did, and therefore his moral culpability is higher than the standard defendant and he deserves more punishment. Finally, Defendant's willingness to spare the government and the public the expense and resources of a trial deserves the 3-level reduction for acceptance of responsibility.

The Court should reject Defendant Serageldin's argument that he should be sentenced as if he had been convicted of 18 U.S.C. § 1924, rather than under the statute for which he was actually convicted: 18 U.S.C. § 793(e).

His argument has two main problems. First, it ignores his significant scheme to obstruct justice. Had the United States not agreed to dismiss the obstruction count on which he was indicted (in exchange for an obstruction-of-justice enhancement guidelines enhancement), his guidelines under the obstruction count would have been an offense level 16, with a sentencing range of 21-27 months.[1] This is already well above the sentence he urges.

Second, Defendant's argument ignores that his offense of conviction, 18 U.S.C. § 793(e), is more serious than the statute he wishes he had been convicted of, 18 U.S.C. § 1924. The elements of § 1924 include only (1) being an employee or contractor of the United States, (2) possessing classified information through that position, (3) knowingly removing that classified information without authority and with intent to retain it at an unauthorized location. *See* 18 U.S.C. § 1924. The elements of § 793(e) with which Defendant Serageldin was charged, on the other hand, include (1) unauthorized possession of national defense information that he had reason could be used to the injury of the United States or to the advantage of a foreign nation, (2) willfully retaining them, and (3) failing to deliver the information to the officer and employee of the United States entitled to receive it after a demand for its return. In other words, even as applied to Defendant Serageldin, a violation of Section 793(e) includes more willful and blameworthy conduct than would a violation of Section 1924. There is therefore no mystery why § 793(e) carries a higher maximum term of punishment (10 years vs. 5 years) and a higher sentencing guideline calculation.

[1] Under USSG § 2J1.2 (Obstruction of Justice), the base offense level is 14, § 2J1.2(a), and that would have been increased by 3 levels for "substantial interference with the administration of justice," § 2J1.2(b)(2), and by an additional 2 levels for obstruction that "involved the selection of . . . especially probative record[s] [and] document[s] . . . to destroy" and that was "otherwise extensive in scope," § 2J1.2(b)(3)(B),(C), then decreased 3 levels down to offense level 16 for acceptance of responsibility. With CHC I, offense level 16 carries a sentencing range of 21 to 27 months.

And Defendant similarly misses several important points when he argues that the guideline for § 793(e) employed here, USSG § 2M3.3, should be ignored because the guideline is inflexible even though § 793(e) covers a broad range conduct, from refusing to return national defense information to transmitting it to another. First, Defendant misses that according to the guidelines' statutory index, § 793(e) can be sentenced under one of two guidelines, depending on the defendant's conduct: under § 2M3.3, as the United States argues here, or under § 2M3.2, *which is 6 offenses levels higher and to be used in cases of willful transmission*, *see* USSG § 2M3.2 n.2. Second, despite § 2M3.3's inflexibility, it still points to an offense level that corresponds to a sentence of 57 to 71 months. In other words, the guidelines are flexible for this offense, they have already given Defendant a break for not committing a § 793(e) offense that involve willful transmission of national defense information, which would be punished more severely under a different guideline, and that even within the § 2M3.3 guideline there are a range of potential sentences.

The Court should therefore sentence Defendant according to the statute under which he was convicted, 18 U.S.C. § 793(e), the sentencing guideline that applies to that statute, USSG § 2M3.3, and the sentencing range that applies to his crime and criminal history category, 57-71 months.

The Sentence

The Supreme Court has directed federal trial courts to initially calculate the appropriate guideline sentencing range under the advisory federal sentencing guidelines. *Gall v. United States*, 552 U.S. 38, 41 (2007). The sentencing guidelines, the Supreme Court has acknowledged, are "the product of careful study based on extensive empirical evidence derived from the review of thousands of individual sentencing decisions." *Id*. at 46 (footnote omitted). The First

Circuit has noted that "the guidelines are the starting point for the fashioning of an individualized sentence, so a major deviation from them must 'be supported by a more significant justification than a minor one.'" *United States v. Martin*, 520 F.3d 87, 91 (1st Cir. 2008) (quoting *Gall*, 552 U.S. at 50).

Thus, the starting point here is the guideline sentencing range specified above: at offense level 25 and criminal history category I, 57-71 months of imprisonment. The United States' recommendation of 60 months – at the low end of that range – is sufficient but not greater than necessary to comply with the purposes of sentencing.

There are no reasons to move off this starting point, as Defendant would have the Court do.

This was no mere technical violation of classified information handling rules: this was a significant breach of national security. The technology largely concerned ballistic missile defense systems, specifically the radar used to detect missiles that are aimed at our soldiers, our ships, our buildings, and our citizens, and to guide our own systems in times of need. Some of the technology was cutting edge, as it involved radar systems that were in the process of being implemented while Defendant was committing his crimes; some of those systems have not been fully implemented yet. And the documents illegally retained were voluminous: approximately 3,137 digital documents recovered on computers, hard drives unattached to computers, thumb drives, and CDs, and another approximately 115 physical documents. Approximately 573 of all these documents were marked as containing classified information, totaling approximately 31,000 pages in length. The documents were long and included specific technical data with diagrams, charts, tables, and formulas. They contained information whose release would benefit

other countries and disadvantage our own. A representative of the Navy will elaborate in a victim impact statement at sentencing.

The danger of exposure to others was significant. Defendant Serageldin kept the documents in or on his car's glove box, his living room, his master bedroom closet, a spare bedroom, the dining room table, a sitting area, a utility room, and even his person. Approximately ten unclassified documents were found on a laptop belonging to his mistress. So even if the Court accepts Defendant's claim that he did not intend to transfer the documents to another, he nevertheless routinely exposed them to his cohabitants and any visitors, and to any foreign observers who might use a breach of security like this to their advantage by breaking into his house or car, or just by carjacking him or mugging him on the street. A dining room table, a shopping bag, and a pants pocket offer little security. And given the number of documents and their disarray, if any had been taken from him by stealth, Defendant would have been hard put to notice.

Why did he have these documents in his home, in his car, and on his person? Defendant has claimed that he was just working on them at home, because he was either a dedicated employee or because he just wanted to avoid the commute. But those contentions miss the point entirely. The whole point of classified information handling rules — which require that classified information be handled, transported, and stored securely — is to protect that information at all times, to avoid jeopardizing its security, and to avoid having to launch an investigation when the information is mishandled. Defendant might claim that he was just careless, maybe a bit of a hoarder. But again, this would miss the point entirely. The procedures are there to protect against the careless and the hoarders: all handlers of classified information learn the procedures when they receive their security clearances, agree to those procedures, and are refreshed on those procedures regularly to ensure compliance. Defendant Serageldin himself received repeated

training on handling classified information. He did not lack the wit or the drive to follow them: he has a Master of Science in scientific computing and a Ph.D. in condensed state of matter, several patents, and speaks four languages.

Moreover, stealing classified information and removing it from secure, authorized storage does not simply create a risk of unauthorized disclosure or access. Rather, as then-Director of the National Security Agency Admiral Michael S. Rogers wrote in an earlier prosecution:

> It is a fundamental mandate in the Intelligence Community that classified material must be handled and stored in very specific and controlled ways. If classified material is not handled or stored according to strict rules, then the government cannot be certain that it remains secret. Once the government loses positive control over classified material, *the government must often treat the material as compromised and take remedial actions as dictated by the particular circumstances. Depending on the type and volume of compromised classified material, such reactions can be costly, time consuming and cause a shift in or abandonment of programs.*

See Ex. C to this sentencing memorandum (Exhibit A to Government's Unclassified Memorandum in Aid of Sentencing, *United States v. Nghia Pho*, Crim. No. GLR-17-631 001 (D. Md. 2018)) (emphasis added). Crimes such as Defendant's can thus trigger costly security-based responses. Moreover, the magnitude, nature, and scope of the defendant's criminal activity caused the United States to expend substantial investigative and analytical resources. Those expenditures were not only financial, but rather also included sought-after experts with rare subject-matter and technical expertise. The diversion of effort by law enforcement and other personnel resulted in significant costs in a variety of manners.

Moreover, there were many red flags that should cause the Court to reject Defendant's contention that he kept these documents at home just so he could work from home:

- Company personnel who reviewed the documents that Defendant took and kept assessed that they appeared to come from mass downloads of complete file directories, rather than selective downloads of specific files;

- The documents included a project that he did not work on, a project that did not involve radar but rather protecting others from tampering with missiles;
- His last two mass downloads occurred on days that were on the weekend and for which he claimed zero work time;
- He altered the classification markings on approximately 50 documents (approximately 1 out of every 11 or 12 classified documents), either by replacing the SECRET or CONFIDENTIAL markings digitally with an "XX" or, on one paper document, by physically cutting off the classification banners with a pair of scissors or a razor blade;
- When confronted, Defendant lied repeatedly over many days about what he had done, tried to avoid returning the documents, and researched how to destroy the evidence, which was thwarted only because of FBI surveillance and the execution of court-ordered search and seizure warrants; and
- Defendant had significant ties abroad.

Defendant's intent to deceive here is corroborated by other instances of deceitful conduct: his time-card fraud (approximately 645 hours fraudulently claimed, which cost his employer over $41,000 in returned contract fees); his home life; his pending criminal charges in state court for unauthorized videotaping; and his violation of stay-away orders in the state and this federal case. In short, any explanation of negligence should be met with distrust. The United States would have made a higher sentencing recommendation if there had been stronger evidence that Defendant had transferred the documents. There is no reason to go below the current recommendation.

Defendant has made two extraordinary claims that should be rejected out of hand. The first is that he removed documents' classification markings in order to create unclassified documents on which he could work at home. This makes no sense whatsoever. Cutting off the classification headers and footers of a classified document does not remove the classified material any more than does cutting the ingredients label off a box of Pop Tarts remove the calories. The second extraordinary claim is that Defendant's multiple ties to Egypt are irrelevant. Of course they are relevant. A defendant like Serageldin with significant ties to a foreign country who has ille-

gally retained national defense information is much more likely to have transferred that information to that foreign country than would a defendant with no foreign ties at all. Moreover, a defendant like Serageldin with significant ties to a foreign country would make a more significant *target* of foreign operatives who might want to steal the documents from an insecure location like Serageldin's home. Either way, his foreign ties are important.

As with so many aspects of national security, the system of protecting national defense information works in large part on the trust placed on those who work in it. It is not enough that they pass background checks. They must also sign agreements, undergo training, undergo retraining, and undergo periodic reinvestigation. But they must also follow the law and, when confronted with a violation, help to correct it, not conceal the violation or seek to destroy evidence of it. Above all, they must not take the information for their or another's advantage, and they must not put the information in harm's way for others to take.

Defendant Serageldin violated all of this. An appropriate sentence is the government's recommendation of 60 months of imprisonment, a fine within the Guidelines sentencing range of $20,000 to $200,000, 36 months of supervised release, a mandatory special assessment of $100, and forfeiture. Such a sentence would be the minimum necessary to reflect the nature and circumstances of this offense, the history and characteristics of Defendant Serageldin, the seriousness of the offense, promote respect for the law, to provide just punishment, and to afford adequate deterrence to others who others who hold the same trust as Defendant once did. *See* 18 U.S.C. § 3553(a).

This sentence would also be consistent with other recent sentences for illegally retaining national defense information in violation of 18 U.S.C. § 793(e). The most comparable is the recent sentence of 66 months of imprisonment for Nghia Hoang Pho, a 68-year-old former em-

ployee of the National Security Agency who violated 18 U.S.C. § 793(e) by taking classified information from the NSA and keeping it at his home. *See* Exhibits A - E (Information, Plea Agreement, Sentencing Exhibit, Judgment, and Press Release for *United States v. Pho,* No. GLR-1-17-CR-00631-001 (D. Md. 2018)). Although Pho's crime was in one aspect more serious because he took information at a higher classification level, Pho's crime was less serious in another aspect because he did not obstruct justice, which Defendant Serageldin did repeatedly. Another comparable sentence is the 41 months of imprisonment for Weldon Marshall, a former member of the Navy who illegally retained documents classified as SECRET about United States nuclear command, control, and communications at his house, including hard drives and laptops. *See* Exhibits F - H (Information, Plea Agreement, and Judgment in *United States v. Marshall,* No. 3:17-CR-00001 (S.D. Tex. 2018)). Marshall's sentence was also within the guidelines, and was lower than the 60-month sentence urged here for Defendant Serageldin because Marshall, unlike Serageldin, did not obstruct justice. Finally, the government's recommendation for Defendant Serageldin is far lower than the *top-of-the-guidelines* 108-month sentence imposed on Harold T. Martin, III, a former member of the Navy for retaining multiple classified documents about various subjects. *See* Exhibits I - K (Indictment, Plea Agreement and Facts, and Judgment in *United States v. Martin,* No. RDB-17-0069 (D. Maryland 2019)). Martin's guideline range was higher than Defendant Serageldin's because Martin took documents at a higher classification level; he did not, however, obstruct justice.

Conclusion

Defendant has asked for a sentence of no imprisonment, because he feels the guidelines are too harsh. Other courts have clearly found the guidelines to be instructive. Defendant has also argued that the guidelines do not take into account that he (purportedly) kept the documents

at home so that he could work on them at home and he (purportedly) did not use them to endanger national security. The guidelines clearly do take this into account. Moreover, he was not a hard worker: he committed time-card fraud. For all the reasons specified above, the Court should reject these arguments.

Defendant Serageldin should be imprisoned and fined and held on supervised release as recommended above, and the Court should deny Defendant's request for a different sentence, especially any sentence that does not include imprisonment.

Respectfully submitted,

ANDREW E. LELLING
United States Attorney

By: */s/ Scott L. Garland*
SCOTT L. GARLAND
Assistant U.S. Attorney

Dated: July 18, 2020

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing and paper copies will be sent to those indicated as non-registered participants on July 18, 2020.

/s/ *Scott L. Garland*
Scott L. Garland
Assistant U.S. Attorney